Microsoft

Hybrid Identity: Azure Active Directory

Joe Losinski
Partner Technology Strategist

Agenda

- Lab (let’s warm up)
- Hybrid Identity Overview
- Active Directory Domain Services (AD DS)
- Azure Active Directory (AAD)
- Azure AD Domain Services (AAD-DS)
- Azure AD Connect
- Azure Active Directory B2C/B2B
- Lab

Microsoft Azure

Lab Setup

https://aka.ms/Pax8

Microsoft Azure

Hybrid Identity Overview

Identity challenges for today's organizations

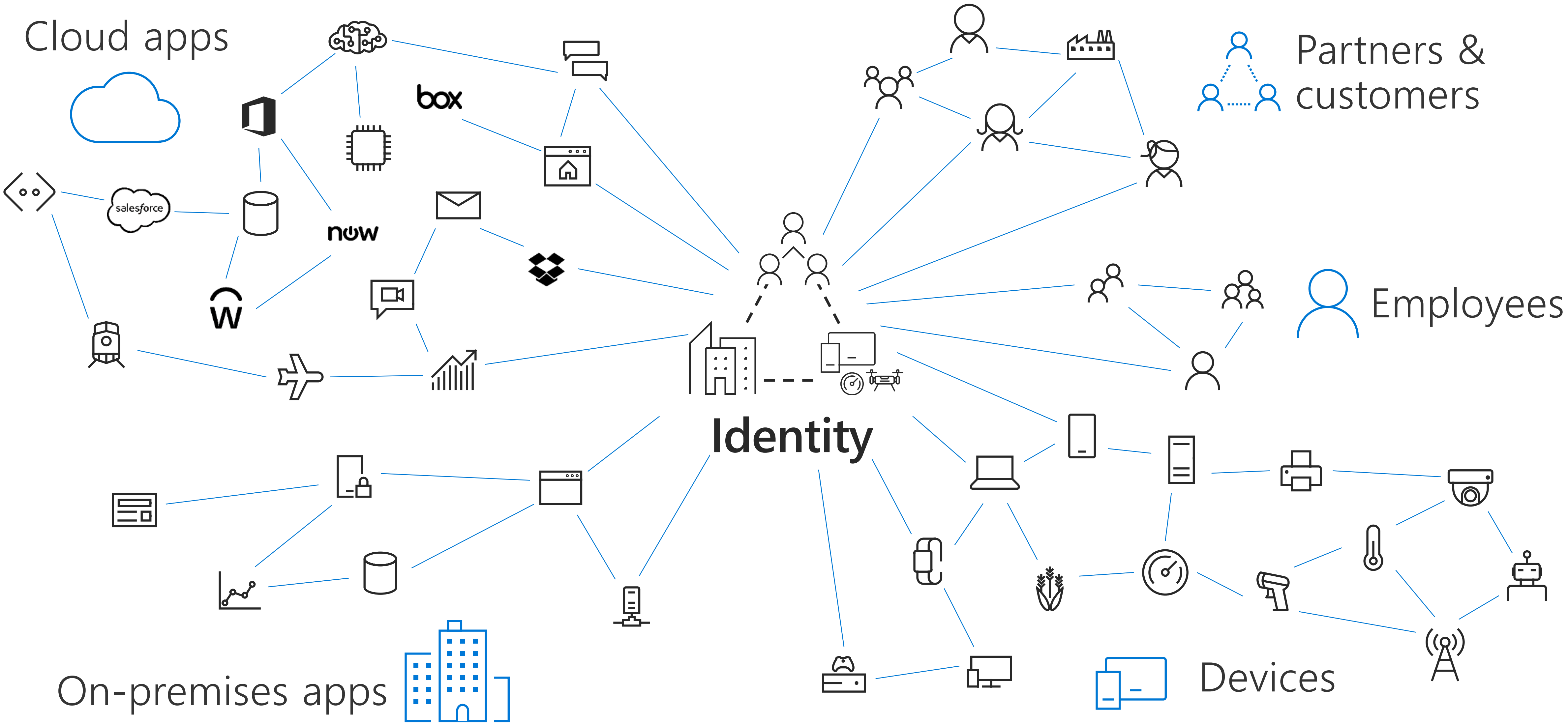
Explosion of apps, devices, and users outside of the corporate network

Increase in identity attacks and lack of visibility and control

Evolving data privacy and security regulations to comply with

Demands for increased productivity and IT modernization

Identity is the new control plane



Microsoft Azure Active Directory

Your universal platform for managing and securing identities

MODERNIZE ACCESS

Connect your users to any app

Single Sign-On
Azure AD Connect
Automated User Lifecycle
Self-Service for End Users
Access from Anywhere

SECURE & GOVERN

Safeguard user credentials

Strong Authentication
Conditional Access
Identity Protection
Privileged Identity Mgmt
Identity Governance

CONNECT & COLLABORATE

Interact with customers and partners

Customer & Partner Identity and Access Management
Cross-Tenant Collaboration
Personalized Customer Journeys
Connect with Any User

DEVELOP & INTEGRATE

Accelerate adoption of your apps

Open standards-based Identity platform
App Integration
Microsoft Graph
Identity for IaaS

Microsoft Azure

Active Directory Domain Services (AD-DS)

Active Directory Domain Services (AD DS)

- Classic on-prem AuthN/AuthZ service available since Server 2000
- 90%+ market penetration
- Provides forests, domains, Organization Units for logical collection and management of objects (computers, users, groups, etc.)
- Requires a domain controller (physical, VM, IaaS VM)
- Primary value-add is group policy and local AuthN/AuthZ
- Granular management of computer and user settings (aka lock down the desktop)

Common Questions

- Can I virtualize a domain controller in an IaaS VM?
- Do I need to get rid of my domain controls on-prem?
- Are domain controllers going away?
- Is Microsoft investing in AD DS?

Microsoft Azure

Azure Active Directory (AAD)

Azure Active Directory in the Marketplace

— Every Office 365 and Microsoft Azure customer uses Azure Active Directory —

14.2M

organizations

+30% YoY

1.01B

identities

+35% YoY

334K

3rd party apps in Azure AD

+150% YoY

64K

paid Azure AD / EMS customers

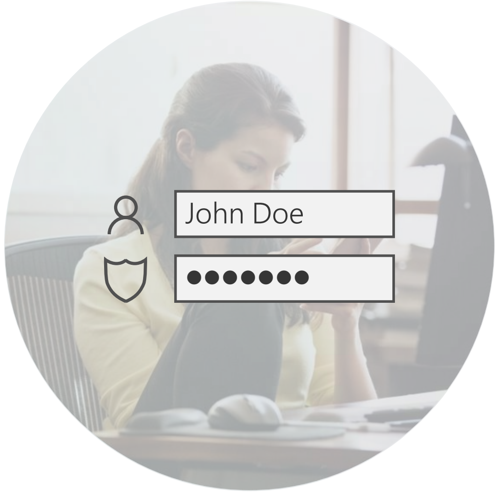
+65% YoY

90%

of Fortune 500 companies use Azure AD

Azure Active Directory

— Identity and access management for employees, partners, and customers —



Provide seamless access

Facilitate collaboration

Unlock IT efficiencies

Enhance security
and compliance

Azure Active Directory

— Identity and access management for employees, partners, and customers —

B2B collaboration

Provisioning-Deprovisioning

Addition of custom cloud apps

Access Panel/MyApps

Dynamic Groups

Identity Protection

Self-Service capabilities

Connect Health

Remote Access to on-premises apps

Azure AD B2C

Group-Based Licensing

Privileged Identity Management

Azure AD Connect

Conditional Access

Microsoft Authenticator - Password-less Access

Azure AD Join

MDM-auto enrollment / Enterprise State Roaming

Security Reporting

SSO to SaaS

Multi-Factor Authentication

Azure AD DS

Office 365 App Launcher

HR App Integration

Access Reviews

Azure Active Directory (AAD)

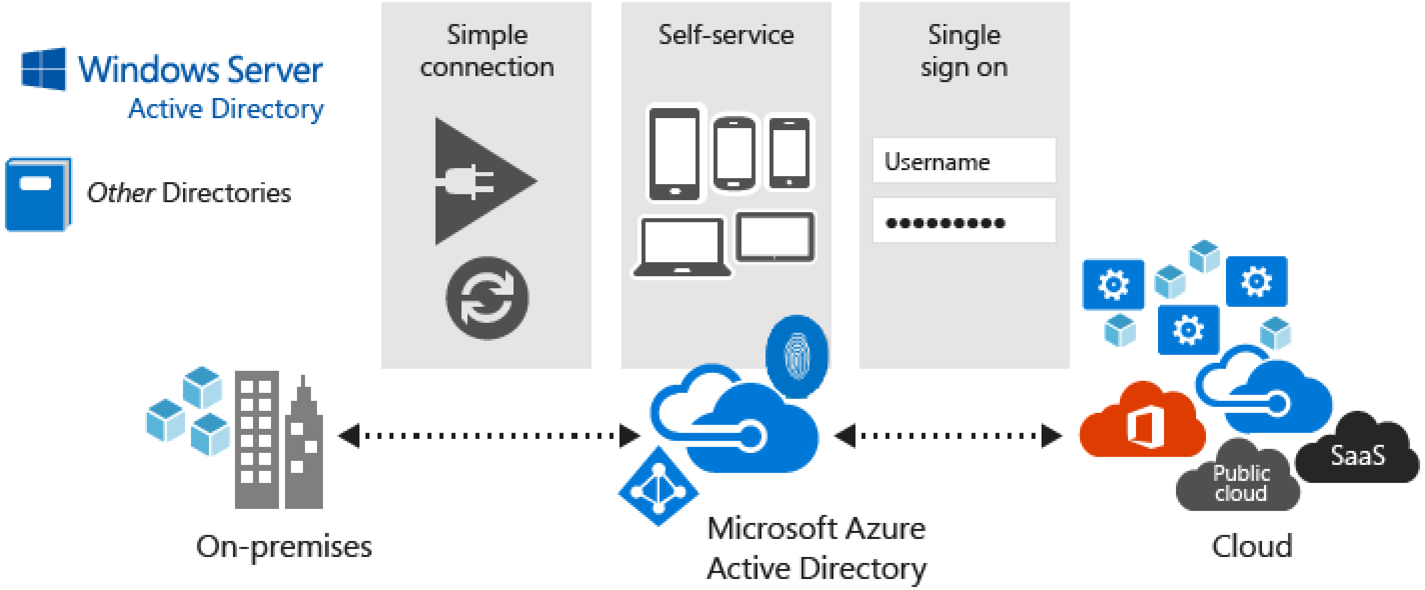
Microsoft's multi-tenant cloud based directory and identity management service

- Comes in four editions
  - Free
  - Basic
  - Premium P1
  - Premium P2
- Users and groups are created in a flat structure without OUs or GPOs
- Authentication is performed through protocols such as SAML, WS-Federation, and OAuth
- https://azure.microsoft.com/en-us/pricing/details/active-directory/

Azure Active Directory (AAD)

Key Features

- Single Sign-On (SSO)
- Self-Service Password Change
- Multi-Factor Authentication (MFA)
- AD Join for Windows 10
- Company Branding



Azure Active Directory (AAD)

AAD is not Active Directory nor Azure Active Directory – Domain Services! One solution does not replace the other …

Most customers will need AD and AAD, and you integrate them with Azure AD Connect

Microsoft Azure

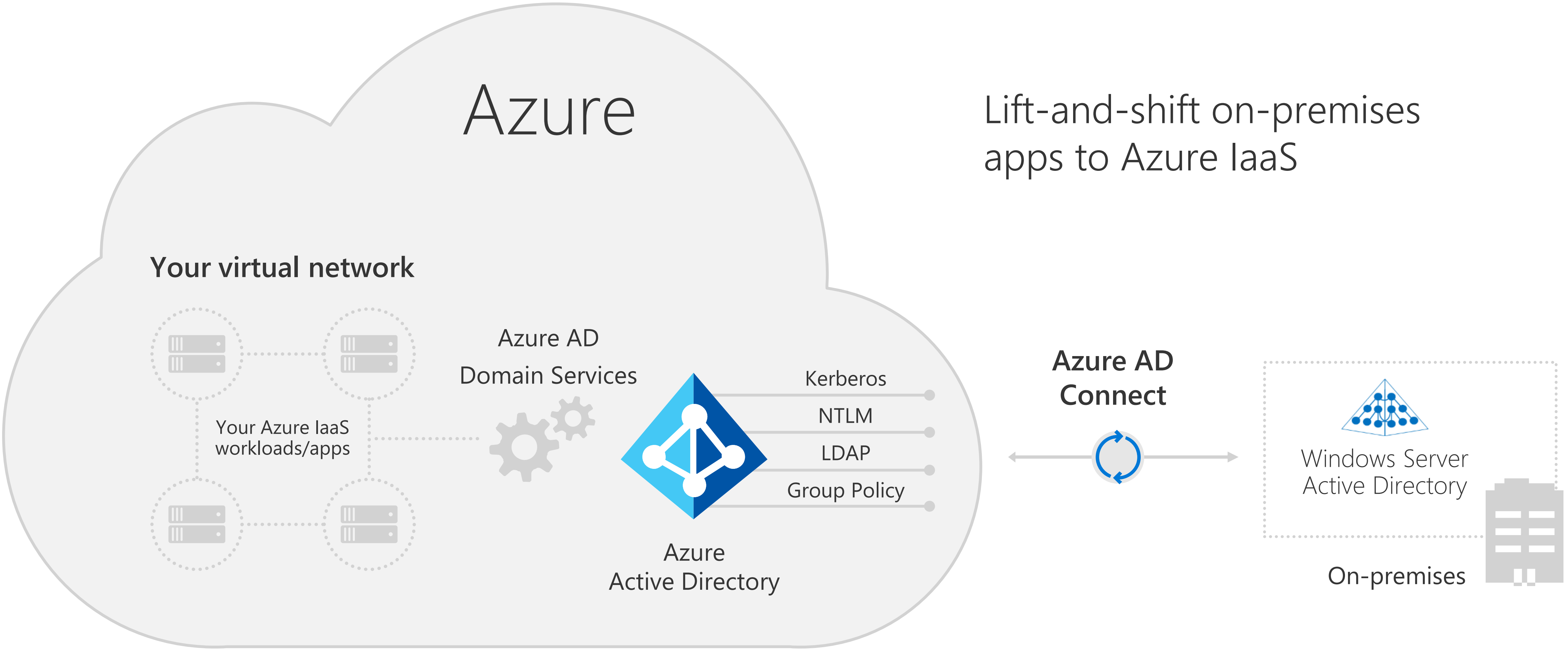
Azure Active Directory – Domain Services (AAD-DS)

Azure AD Domain Services

- AD DS evolved to the cloud
- Provides managed domain services such as domain join, group policy, LDAP, Kerberos/NTLM authentication that are fully compatible with Windows Server Active Directory
- Enables you to deploy your workloads in Azure Infrastructure Services without having to worry about maintaining your identity infrastructure
- Great for cloud-only customers that do not have any on-premises identity footprint

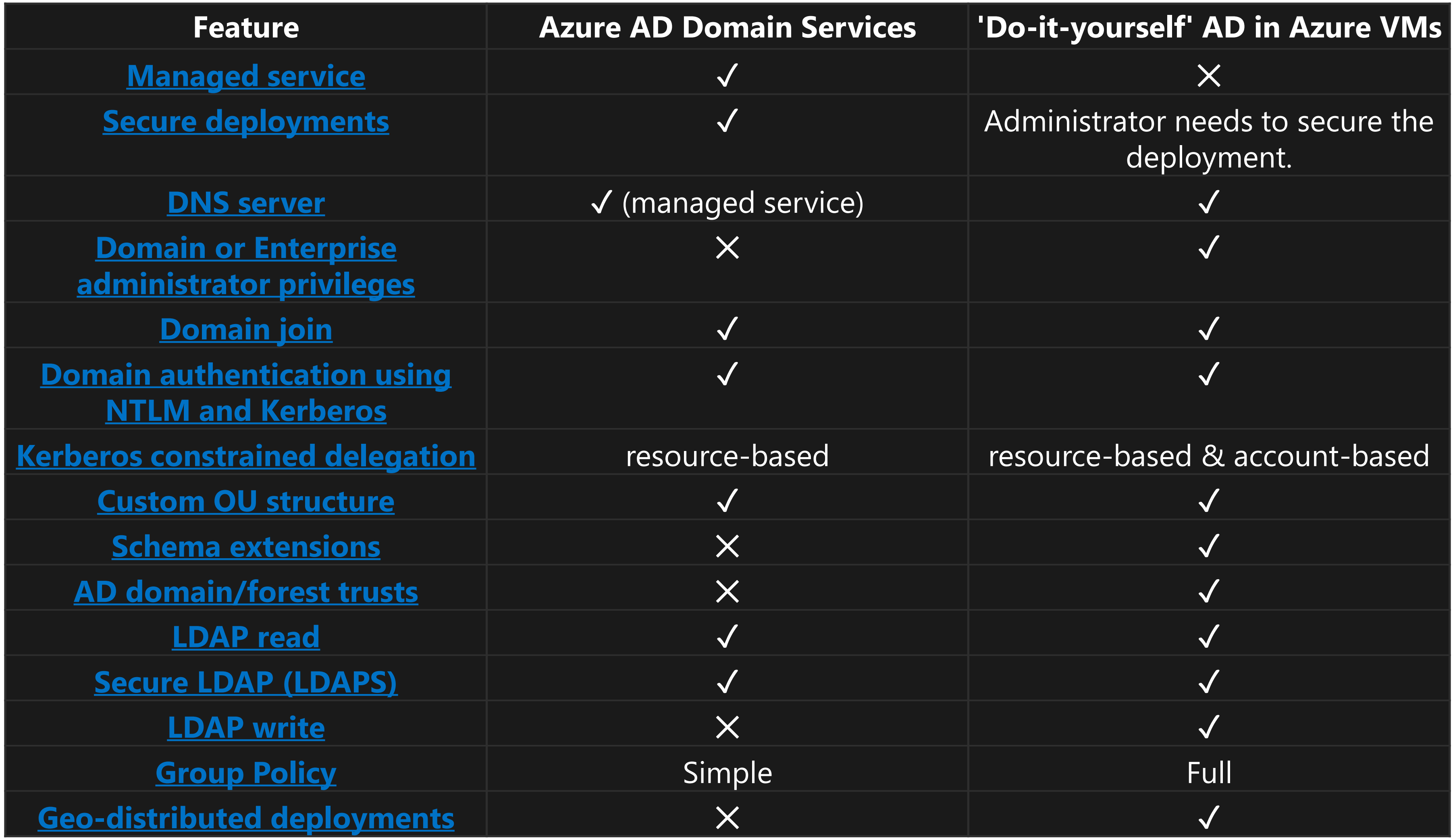
Azure Active Directory Domain Services

Lift-and-shift on-premises apps to Azure IaaS



Azure AD Domain Services

- Key differentiators



Feature	Azure AD Domain Services	'Do-it-yourself' AD in Azure VMs
Managed service	✓	✕
Secure deployments	✓	Administrator needs to secure the deployment.
DNS server	✓ (managed service)	✓
Domain or Enterprise administrator privileges	✕	✓
Domain join	✓	✓
Domain authentication using NTLM and Kerberos	✓	✓
Kerberos constrained delegation	resource-based	resource-based & account-based
Custom OU structure	✓	✓
Schema extensions	✕	✓
AD domain/forest trusts	✕	✓
LDAP read	✓	✓
Secure LDAP (LDAPS)	✓	✓
LDAP write	✕	✓
Group Policy	Simple	Full
Geo-distributed deployments	✕	✓

Microsoft Azure

AD Connect

Azure AD Connect

Integrate your on-premises directories with Azure Active Directory allowing a common identity for Office 365, Azure, and SaaS applications integrated with Azure AD

Made up of three primary components:

1. synchronization services

responsible for creating users, groups, and other objects. It is also responsible for making sure identity information for your on-premises users and groups is matching the cloud

2. monitoring component named [Azure AD Connect Health]

robust monitoring and provide a central location in the Azure portal to view this activity

3. optional Active Directory Federation Services component

used to configure a hybrid environment using an on-premises AD FS infrastructure. This can be used by organizations to address complex deployments, such as domain join SSO, enforcement of AD sign-in policy, and smart card or 3rd party MFA.

Azure AD Connect

Optional Features:
Filtering is used when you want to limit which objects are synchronized to Azure AD. Password synchronization synchronizes the password hash in Active Directory to Azure AD.

Password writeback will allow your users to change and reset their passwords in the cloud and have your on-premises password policy applied.

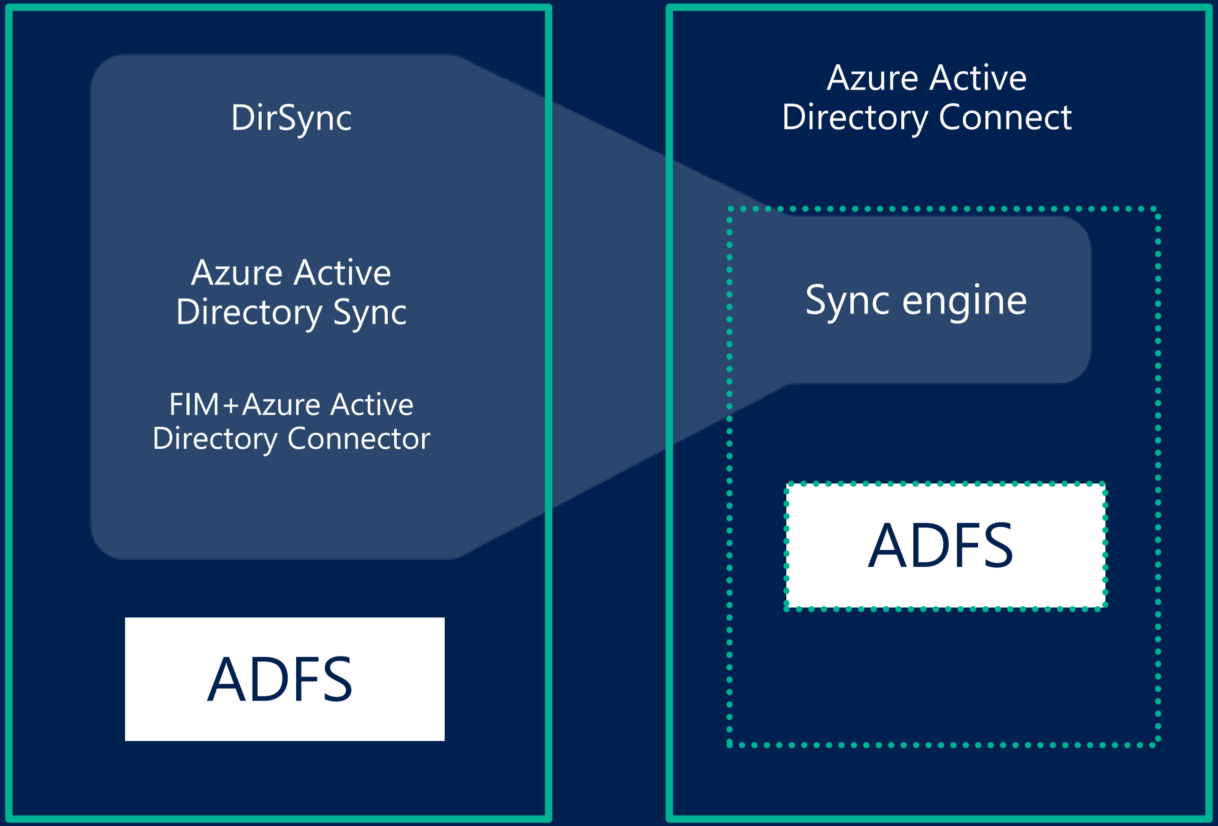
Device writeback will allow a device registered in Azure AD to be written back to on-premises Active Directory so it can be used for conditional access.

Prevent accidental deletes feature is turned on by default and protects your cloud directory from numerous deletes at the same time. Automatic upgrade is enabled by default for express settings installations and ensures your Azure AD Connect is always up to date with the latest release.

1000s OF APPS, 1 IDENTITY

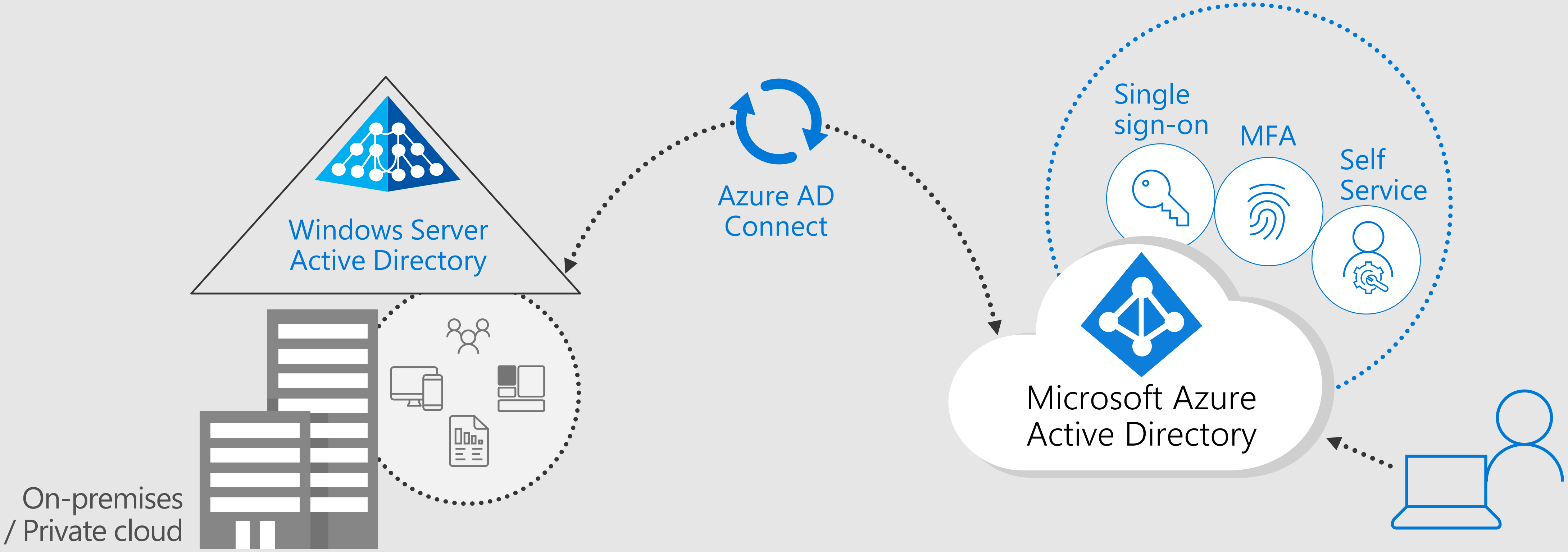
Making a hybrid identity simple

Azure Active Directory Connect


DirSync
Azure Active Directory Sync
FIM+Azure Active Directory Connector
ADFS
Azure Active Directory Connect
Sync engine
ADFS

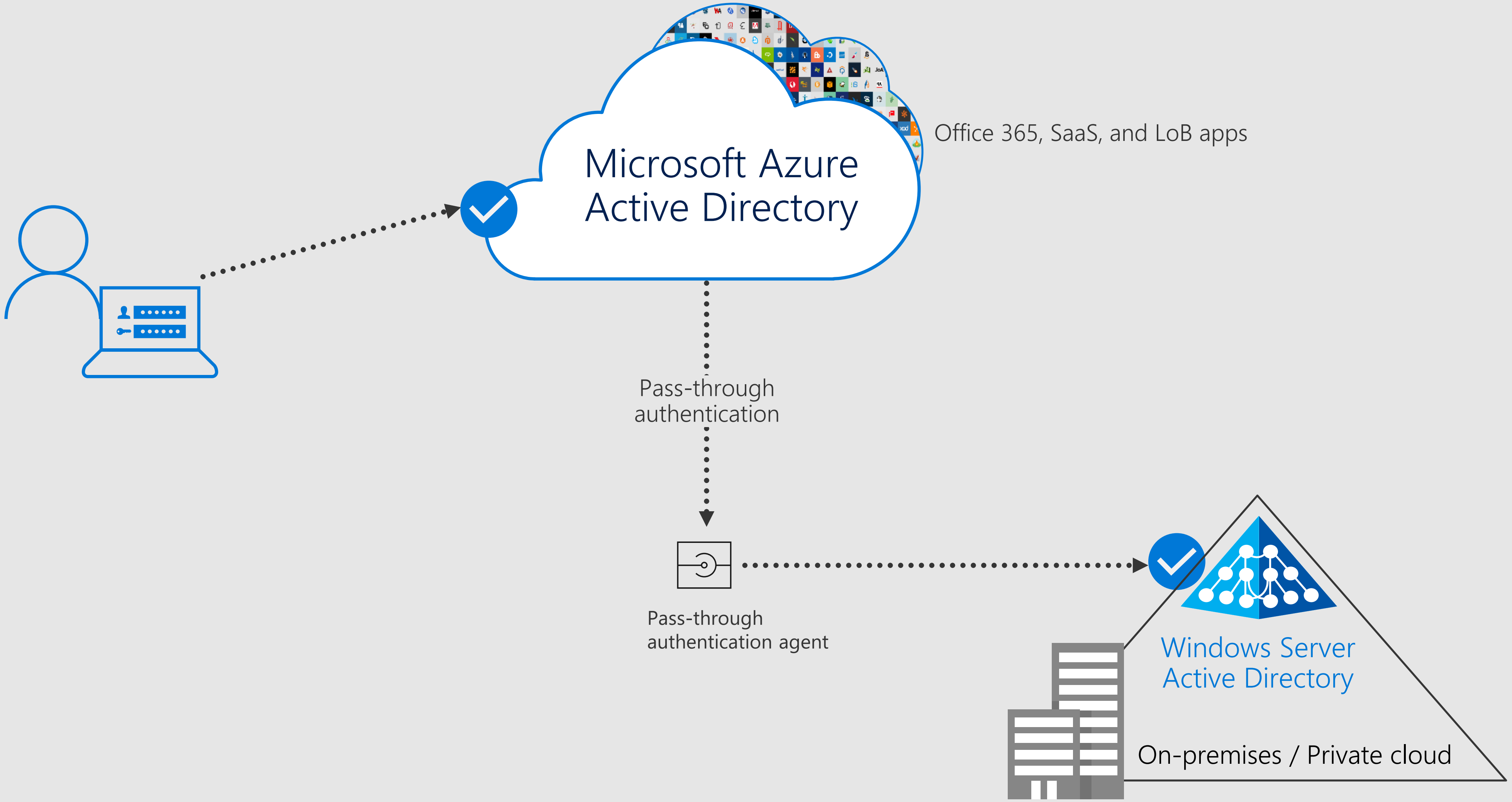
- Consolidated deployment assistant for your identity bridge components.
- All currently available sync engines will be replaced by the sync engine included in the Connect tool.
  Assisted deployment of ADFS will be available through Azure Active Directory Connect.
- ADFS is an optional component for authentication in hybrid implementation. Password sync can replace ADFS for more scenarios.

Hybrid made easy



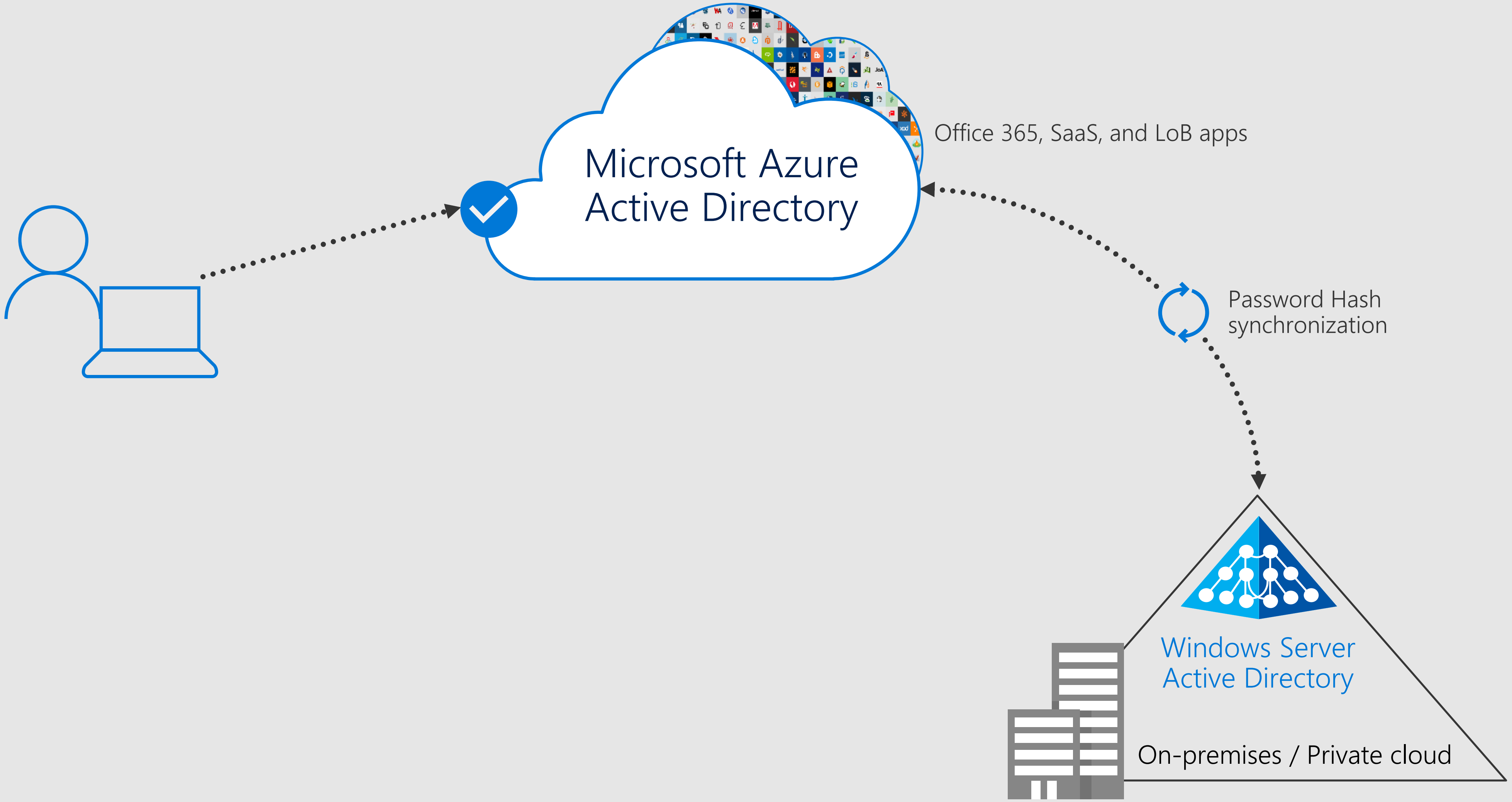
Azure AD Connect authentication options

Pass-through authentication



Azure AD Connect authentication options

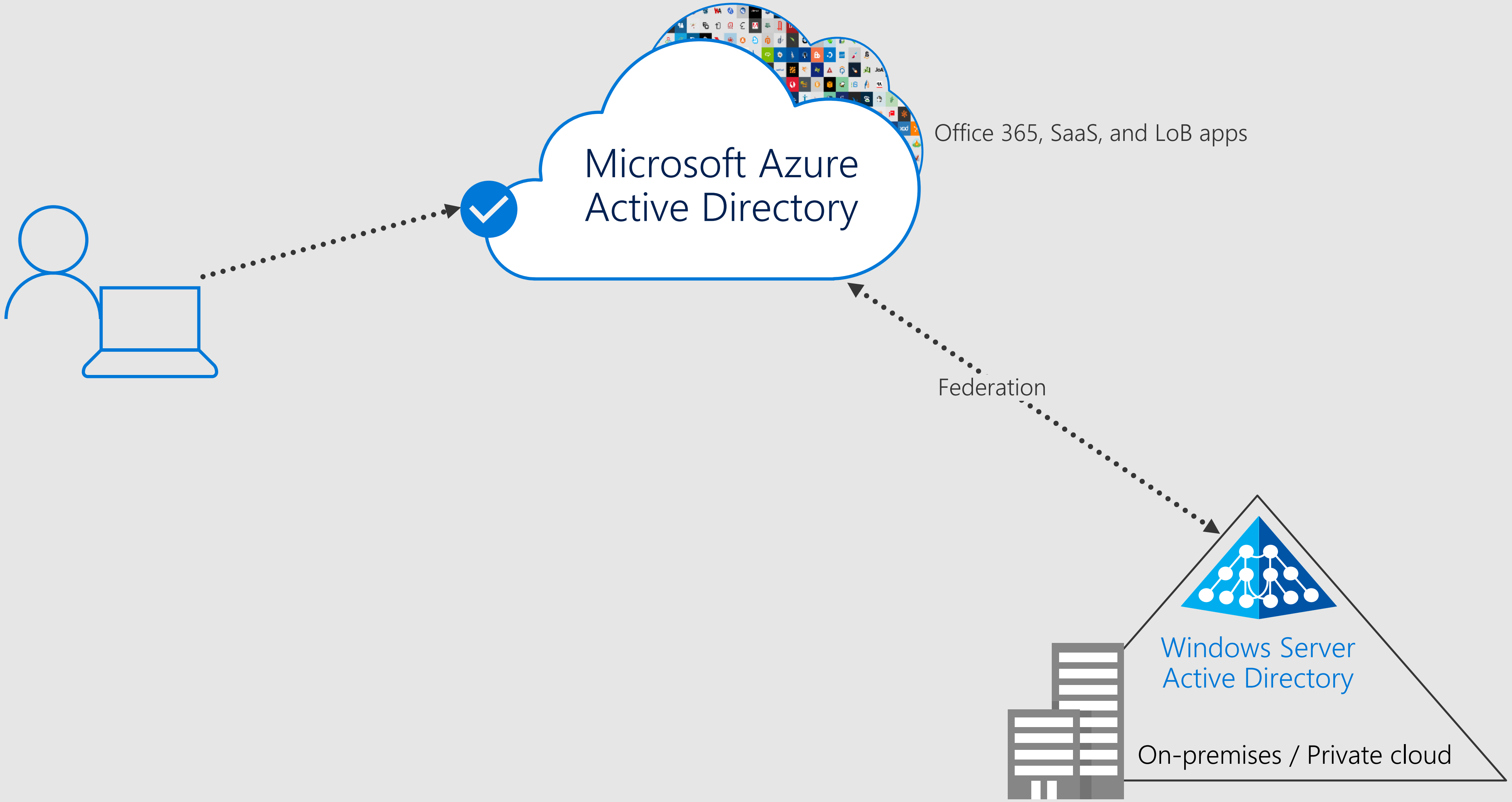
Password Hash synchronization



Office 365, SaaS, and LoB apps
Microsoft Azure Active Directory
Password Hash synchronization
Windows Server Active Directory
On-premises / Private cloud

Azure AD Connect authentication options

Federation via ADFS


Microsoft Azure Active Directory
Office 365, SaaS, and LoB apps
Federation
Windows Server Active Directory
On-premises / Private cloud

Microsoft Azure

Azure AD B2B
Azure AD B2C

Azure Active Directory B2B collaboration

Work with any user from any partner

Partners use their own credentials

No requirement for partners to use Azure AD

No external directories or complex set-up required

Simple and secure collaboration

Provide access to any corporate app or data

Seamless user experiences

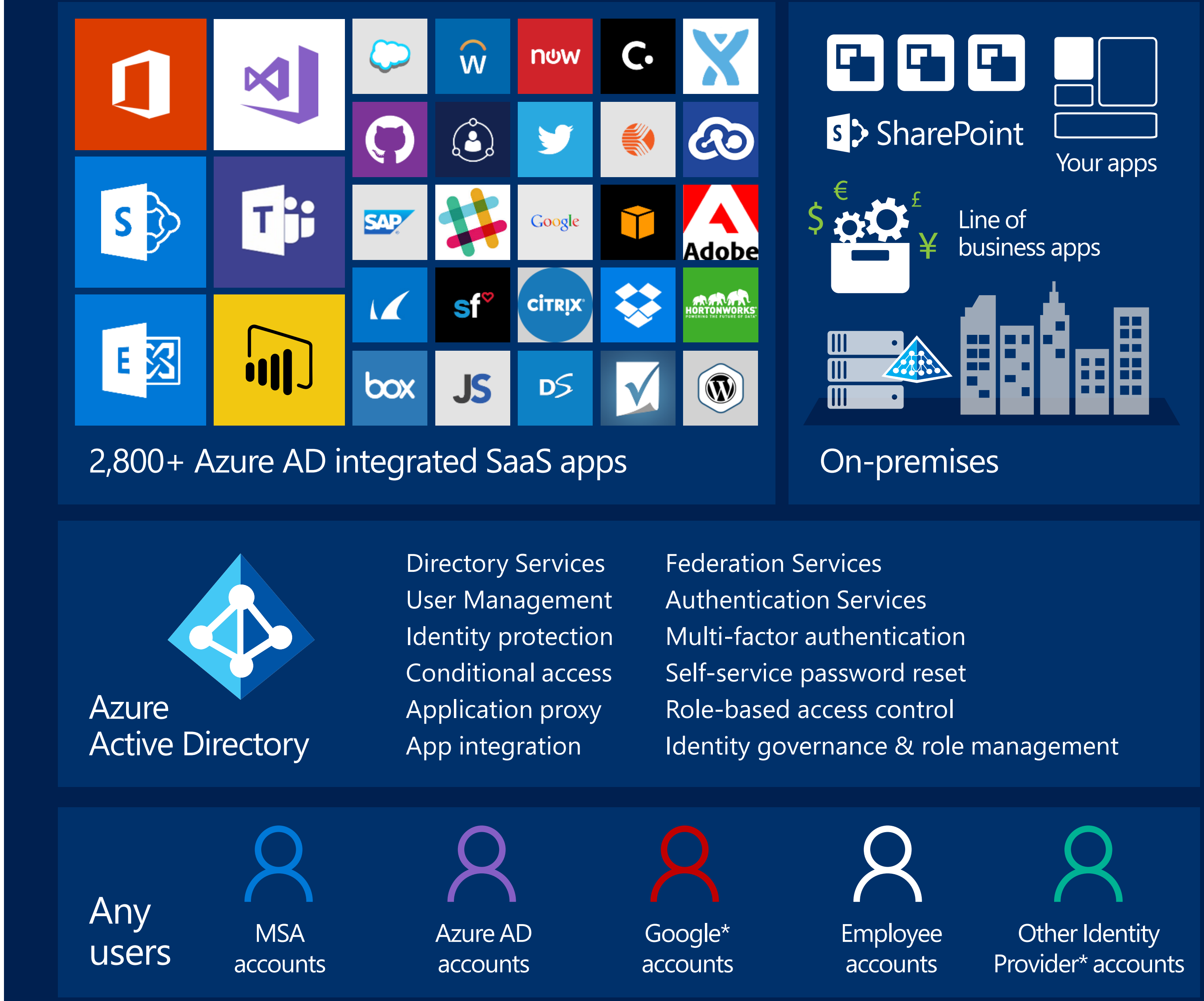
Enterprise-grade security for apps and data

No management overhead

No external account or password management

No sync or manual account lifecycle management

No external administrative overhead



2,800+ Azure AD integrated SaaS apps

SharePoint

Your apps

Line of business apps

On-premises

Azure Active Directory

Directory Services
User Management
Identity protection
Conditional access
Application proxy
App integration

Federation Services
Authentication Services
Multi-factor authentication
Self-service password reset
Role-based access control
Identity governance & role management

Any users

MSA accounts

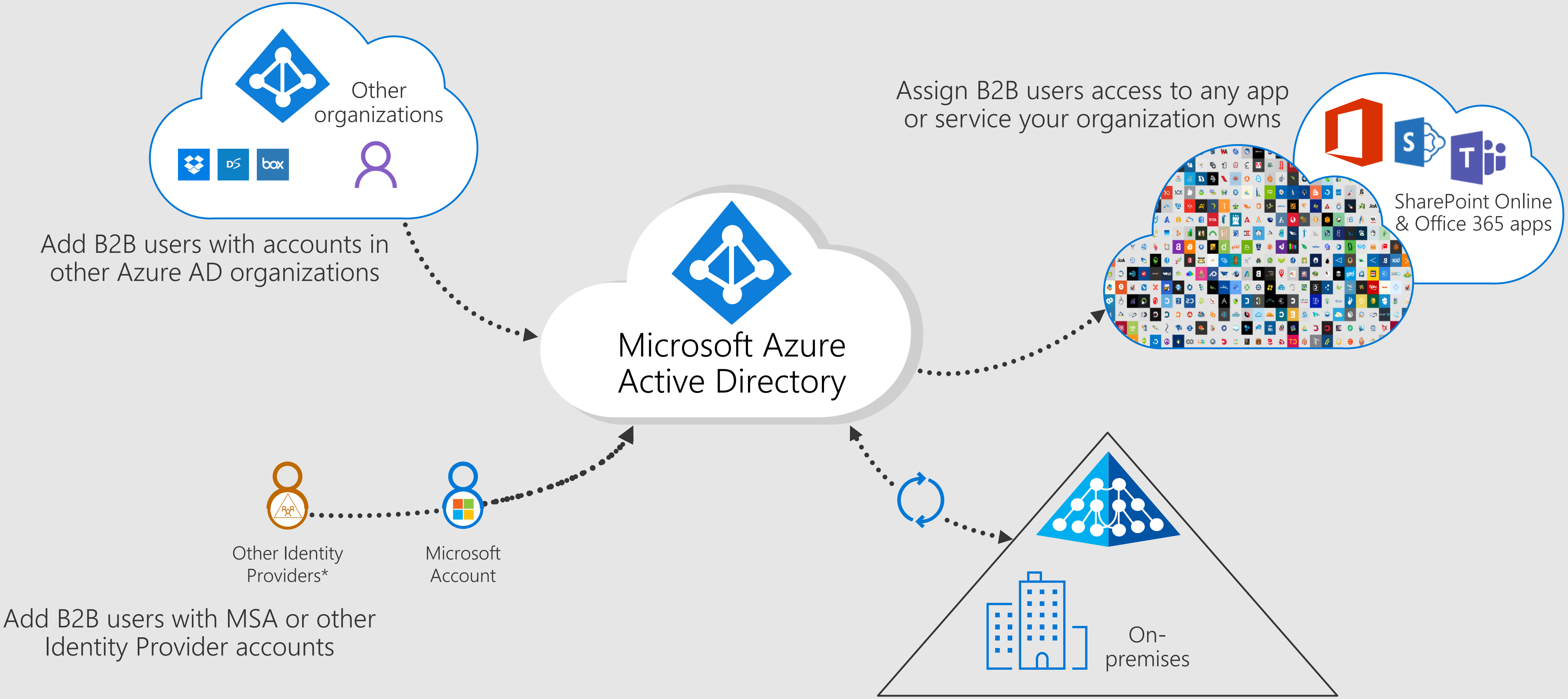
Azure AD accounts

Google* accounts

Employee accounts

Other Identity Provider* accounts

Azure AD B2B collaboration



Other organizations

Add B2B users with accounts in other Azure AD organizations

Microsoft Azure Active Directory

Assign B2B users access to any app or service your organization owns

SharePoint Online & Office 365 apps

Other Identity Providers*

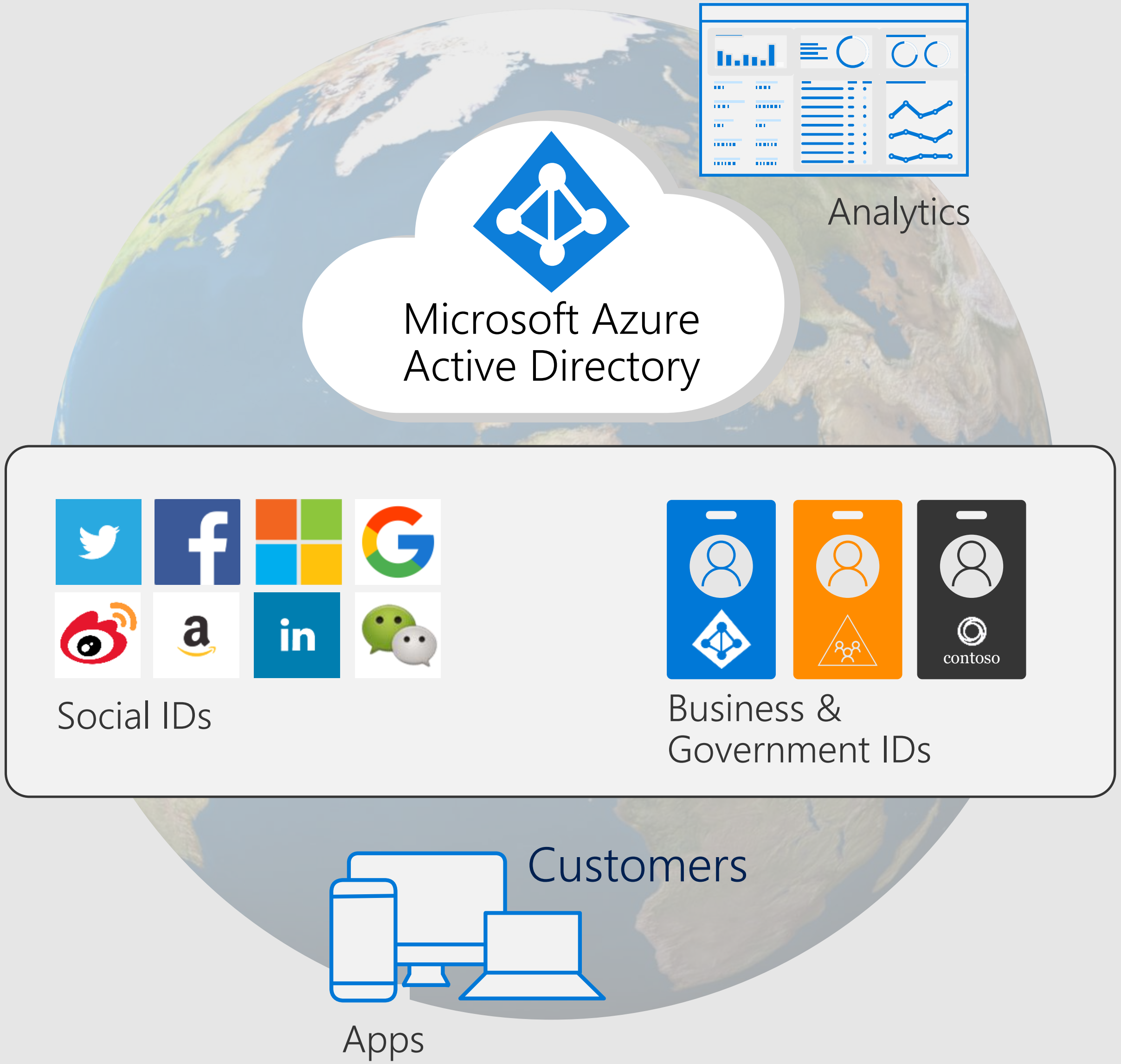
Microsoft Account

Add B2B users with MSA or other Identity Provider accounts

On-premises

Azure Active Directory B2C

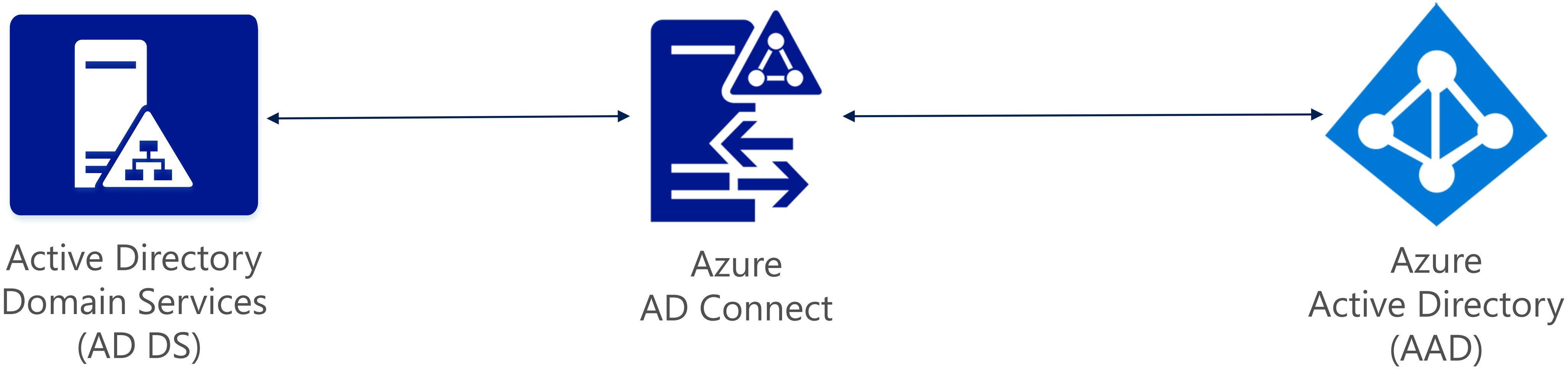
- Securely authenticate your customers using their preferred identity provider
- Capture login, preference, and conversion data for customers
- Provide branded (white-label) registration and login experiences



Microsoft Azure

Lab Architecture

Lab Architecture


Active Directory
Domain Services
(AD DS)
Azure
AD Connect
Azure
Active Directory
(AAD)